Chicago Police Department

General Order G09-01-06

USE OF SOCIAL MEDIA OUTLETS

ISSUE DATE:	07 August 2014	**EFFECTIVE DATE:**	07 August 2014
RESCINDS:	9 March 2012 version		
INDEX CATEGORY:	Information Management		

I. PURPOSE

This directive establishes guidelines and responsibilities of Department members using social media outlets.

II. SCOPE

For the purposes of this directive, the term "social media outlets" means any electronic communication (such as personal Web sites and outlets for social networking and microblogging) through which participants utilize online communities to share information, ideas, personal messages, and other content through an electronic format. These formats include, but are not limited to, text, video, photographs, audio, digital documents, etc.

This directive addresses the full breadth and scope of social media rather than any one particular format. The Department recognizes that as technology advances, new methods for social media participation will emerge.

III. POLICY

Social media outlets, when used in a proper manner, can reinforce the Department's relationship with the public, build community support, and assist in solving crime. Department members have a constitutional right to express their views under the First Amendment. However, Department members may be subject to discipline for violating the provisions of this directive. Any social media participation made pursuant to a Department member's official duties is not considered protected speech under the First Amendment.

IV. DEPARTMENT SOCIAL MEDIA OUTLETS

A. Procedures

1. All Department social media outlets shall be approved by the Superintendent or his/her designee and shall be administered by Public Safety Information Technology (PSIT).
2. The use of Department computers by Department members to access any social media outlet is prohibited absent prior supervisory approval.
3. Social media content shall adhere to applicable laws, the **Rules and Regulations of the Chicago Police Department**, and any relevant Department policies, including all information technology and records management policies.
   a. Department records retention schedules shall apply to social media content.
   b. Content is subject to Local Records Act (50 ILCS 205/1).
   c. Content must be managed, stored, and retrievable in compliance with the Illinois Freedom of Information Act (5 ILCS 140/1) and any relevant Department directives.

B. Department members authorized to administer Department social media outlets shall:

1. conduct themselves at all times as representatives of the Department and, accordingly, shall adhere to applicable Department Rules and Regulations and Department directives.
2. not make statements indicating the guilt or innocence of any suspect or arrestee, or comments concerning pending prosecutions.

3. not post, transmit, or otherwise disseminate confidential information related to Department training, activities, or on-going investigations without express written permission.

4. comply with all copyright, trademark, and service mark restrictions in posting materials to electronic media.

5. not use personally owned devices to manage the Department's social media activities without proper approval.

6. ensure that all relevant privacy protections are maintained.

V. DEPARTMENT MEMBERS' PERSONAL USE OF SOCIAL MEDIA OUTLETS

A. When using social media, Department members should be mindful that their communications become part of the worldwide electronic public domain. Department members should be aware that privacy settings and social media sites are subject to constant modifications, and they should never assume that personal information posted on such sites is protected or secure.

B. Department members should expect that any information that they create, transmit, download, exchange, or discuss that is available online in a public forum may be accessed by the Department without prior notice.

C. Department members are prohibited from posting, displaying, or transmitting:

1. any communications that discredit or reflect poorly on the Department, its missions or goals.

2. content that is disparaging to a person or group based on race, religion, sexual orientation, or any other protected class.

3. Department information, records, documents, video recordings, audio recordings, or photographs to which they have access as a result of their employment without the written permission from the Office of News Affairs or the Office of the Superintendent.

4. any references to any other Department member's employment by the Department without that person's consent.

5. any intellectual property of the Department or the City of Chicago without the specific authorization of the Superintendent or his/her designee. Department or City of Chicago intellectual property includes but is not limited to logos, uniforms, official photographs, audio/ video files, or any text documents (paper or electronic).

6. *any information representing themselves as an official spokesperson of the Department and the City of Chicago unless specifically authorized by the Superintendent or his/her designee.*

VI. USE OF SOCIAL MEDIA OUTLETS FOR INVESTIGATIVE PURPOSES

A. *Social media is a valuable investigative tool when seeking evidence or information about:*

1. *missing persons;*

2. *wanted persons;*

3. *gang participation and retaliation;*

4. *crimes perpetrated online (i.e., cyberbullying, cyberstalking); and*

5. *photos or videos of a crime posted by a participant or observer.*

B. *Department members utilizing a social media outlet as an investigative tool will:*

1. *use only Department electronic equipment throughout the investigation.*

2. *conduct an investigation only while on duty.*

3. *follow the guidelines set forth in the Rules and Regulations of the Chicago Police Department and the Department directives including, but not limited to, "**Use of the Internet**" and "**Department-Issued Electronic Communication Devices.**"*

4. *only use publicly available open source material.*

3. not post, transmit, or otherwise disseminate confidential information related to Department training, activities, or on-going investigations without express written permission.

4. comply with all copyright, trademark, and service mark restrictions in posting materials to electronic media.

5. not use personally owned devices to manage the Department's social media activities without proper approval.

6. ensure that all relevant privacy protections are maintained.

V. DEPARTMENT MEMBERS' PERSONAL USE OF SOCIAL MEDIA OUTLETS

A. When using social media, Department members should be mindful that their communications become part of the worldwide electronic public domain. Department members should be aware that privacy settings and social media sites are subject to constant modifications, and they should never assume that personal information posted on such sites is protected or secure.

B. Department members should expect that any information that they create, transmit, download, exchange, or discuss that is available online in a public forum may be accessed by the Department without prior notice.

C. Department members are prohibited from posting, displaying, or transmitting:

1. any communications that discredit or reflect poorly on the Department, its missions or goals.

2. content that is disparaging to a person or group based on race, religion, sexual orientation, or any other protected class.

3. Department information, records, documents, video recordings, audio recordings, or photographs to which they have access as a result of their employment without the written permission from the Office of News Affairs or the Office of the Superintendent.

4. any references to any other Department member's employment by the Department without that person's consent.

5. any intellectual property of the Department or the City of Chicago without the specific authorization of the Superintendent or his/her designee. Department or City of Chicago intellectual property includes but is not limited to logos, uniforms, official photographs, audio/video files, or any text documents (paper or electronic).

6. *any information representing themselves as an official spokesperson of the Department and the City of Chicago unless specifically authorized by the Superintendent or his/her designee.*

VI. USE OF SOCIAL MEDIA OUTLETS FOR INVESTIGATIVE PURPOSES

A. *Social media is a valuable investigative tool when seeking evidence or information about:*

1. *missing persons;*

2. *wanted persons;*

3. *gang participation and retaliation;*

4. *crimes perpetrated online (i.e., cyberbullying, cyberstalking); and*

5. *photos or videos of a crime posted by a participant or observer.*

B. *Department members utilizing a social media outlet as an investigative tool will:*

1. *use only Department electronic equipment throughout the investigation.*

2. *conduct an investigation only while on duty.*

3. *follow the guidelines set forth in the Rules and Regulations of the Chicago Police Department and the Department directives including, but not limited to, "Use of the Internet" and "Department-Issued Electronic Communication Devices."*

4. *only use publicly available open source material.*

C. *Department members utilizing a social media outlet as an investigative tool will not:*

1. *use their personal social media account or personal account information to access the social media content.*

2. *use another individual's personal account without his/her consent and the approval of their Bureau Chief.*

3. *actively participate in any discussion or contact with a suspect using alias account information without the authorization of the Chief, Bureau of Organized Crime, or designee.*

   NOTE: *Prior authorization to access information on publicly available internet sources is not required.*

4. *create an alias account or identity without the authorization of the Chief, Bureau of Organized Crime or their designee.*

(Items indicated by *italics/double underline* were revised.)

Garry F. McCarthy
Superintendent of Police

14-081 RWN

Chicago Police Department

Special Order S02-03-10

SOCIAL MEDIA OUTLET: TWITTER

ISSUE DATE:	18 April 2016	**EFFECTIVE DATE:**	18 April 2016
RESCINDS:	15 May 2013 Version of D13-07		
INDEX CATEGORY:	Human Rights and Community Partnerships		

I. PURPOSE

This directive *establishes Department policy and procedures to create, maintain, and publish text based messages to the* Chicago Police Department Twitter *account.*

II. SOCIAL MEDIA OUTLET: TWITTER

A. Twitter is an online social networking and microblogging service that enables its users to send and read text-based messages known as "tweets."

B. Twitter is a means to connect the Department to the community in real time. The Department uses Twitter as a tool to build relationships with community members.

III. GENERAL INFORMATION

A. The Chicago Police Department is committed to serving the community and recognizes that current technology, when utilized properly, can provide the Department and community with an essential channel of communication.

B. *Each District should have a Twitter presence and should be disseminating the following types of information: community alerts, crime prevention tips, success stories and community events.*

C. *Volunteer members should be police officers with authority from the District Commanders to disseminate information on behalf of the district.* Volunteer members will participate in the program **only** during on-duty hours and will not receive additional compensation for participating in the program.

D. The identified volunteer members in each district will maintain and update the district-specific authorized Twitter account and use the account to communicate with and engage members of the community in this casual forum.

IV. GUIDELINES

A. *Information posted on Twitter often results in media inquires. District personnel shall:*

1. *notify the Office of News Affairs of tweets concerning notable incidents (e.g. newsworthy arrests)* ***prior*** *to dissemination.*

2. *direct all media inquiries received regarding district-specific Twitter postings to the Office of News Affairs.*

B. The identified volunteer members will be acting as an official representative of the Department and are expected to act accordingly.

C. *Twitter postings should provide information specific to the participating member's district.*

D. Those members authorized to post district-specific Twitter entries/responses will do so using only a Department electronic device.

E. Unauthorized advertising of private projects, products or services will not be allowed.

F. Participating members must follow the guidelines set forth in the **Rules and Regulations of the Chicago Police Department** and the Department directives including, but not limited to, "**Use of**

Social Media Outlets," "**Use of the Internet**," and "**Department-Issued Electronic Communication Devices**."

V. PROCEDURES

A. District commanders will:

1. identify two members to function as the district Twitter representatives.
2. submit the names, ranks, star numbers, employee numbers, log-on ID numbers and Department e-mail addresses of the Twitter representatives to the Office of News Affairs.

B. The district community policing sergeant will review the respective district-specific Twitter postings on a regular basis and ensure:

1. *those making the District's Twitter account entries post district crime alerts, crime prevention tips, district beat meetings, district success stories and special events.*
2. that any posted information is current, correct, valid, and appropriate.
3. that any posting deemed inappropriate is discontinued.

C. Office of News Affairs will:

1. *provide participating members with social media guidance.*
2. *respond to any media inquiries that result from District-level Twitter communications.*
3. oversee the Twitter account transmissions.

D. *Information Services Division* will be responsible for:

1. any technical aspects of the program.
2. ensuring the program is in compliance with all record retention requirements.

VI. CONFLICT PROVISION

If this directive conflicts with the existing policy concerning the use and prohibitions of social media or acting as an official representative of the Department, including the policies outlined in Department directives entitled "**Use of Social Media Outlets**," "**Use of the Internet**," and "**News Media Guidelines**," this directive will take precedence.

Authenticated by: KC

Eddie T. Johnson
Superintendent of Police

15-156 SDR

DEPLOYMENT OPERATIONS CENTER Special Order	Date of Issue 8 April 2015	Effective Date 9 April 2015	No. 15-01
Subject SOCIAL MEDIA POLICY		Amends	
Related Directives		Rescinds	

I. Purpose

The Deployment Operations Center (DOC)/Crime Prevention and Information Center (CPIC) endorses the secure use of *publically available* social networking sites (SNSs) to assist the fusion center in providing situational awareness, investigate and prevent criminal incidents and establish a common operating picture for federal, state, local, and tribal governments, and to enhance investigations, as appropriate. This policy establishes the DOC/CPIC's position on the management and use of *publically available* social networking sites and provides guidance on its administration and oversight. This policy does not address one particular form of publically available social networking site; rather social networking sites in general.

II. Policy

The DOC/CPIC recognizes that social networking sites have become useful tools for public and law enforcement entities and that criminal offenders frequently utilize these sites for illegal purposes. Harnessing social media tools and resources can be used to prevent, mitigate, respond to, and investigate criminal activity and assist in numerous other public safety functions. This policy provides guidance and protocol in addition to information of a precautionary nature as well as prohibitions on the use of social networking sites by members.

The DOC/CPIC will use internet-based platforms that provide a variety of ways to follow activity related to monitoring publicly available online forums, blogs, public websites, and message boards. Through the use of publicly available search engines and content aggregators, the CPIC fusion center will monitor activities on the social media sites for information that the fusion center can use to provide situational awareness, assist with the Center's public safety mission, prevent terrorism, and assist in criminal investigations and criminal prevention. The DOC/CPIC and its members are aware that social media provides a new forum for free speech but also introduce a potential risk to individuals' privacy, civil rights, and civil liberties if unauthorized or inappropriate access or use occurs. The DOC/CPIC and its members will continue to protect individuals' privacy, civil rights and civil liberties despite the abundance of social media sites and new technology.

III. Definitions

"Social Networking" is defined as social network sites that use Internet services to allow individuals to construct a public or semi-public profile within that system. In some cases individuals may define a list of other users with whom they share some connection, and view and access their list of connections and those made by others within that system. The type of network and its design vary from site to site.

- *Blog:* Short for "Web Log," this term refers to a list of journal entries posted on a Web page. Anybody who knows how to create and publish a Web page can publish their own blog. Some Web hosts have made it even easier by creating an interface where users can simply type a text entry and hit "publish" to publish their blog.

- *Page:* The specific portion of a social media website where content is displayed, and managed by an individual or individuals with administrator rights.

- Post: Content an individual shares on a social media site or the act of publishing content on a site.

- Profile: Information that a user provides about himself or herself on a social networking site.

- Social Media: A category of Internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social networking sites (Facebook, MySpace), microblogging sites (Twitter, Nixle), photo- and videosharing sites (Flickr, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit).

- Social Networks: Online platforms where users can create profiles, share information, and socialize with others using a range of technologies.

- Speech: Expression or communication of thoughts or opinions in spoken words, in writing, by expressive conduct, symbolism, photographs, videotape, or related forms of communication.

- Web 2.0: Web 2.0 is term that was introduced in 2004 and refers to the second generation of the World Wide Web. The term "2.0" comes from the software industry, where new versions of software programs are labeled with an incremental version number. Like software, the new generation of the Web includes new features and functionality that was not available in the past. However, Web 2.0 does not refer to a specific version of the Web, but rather a series of technological improvements.

-Wiki: A wiki is a Web site that allows users to add and update content on the site using their own Web browser. This is made possible by Wiki software that runs on the Web server. Wikis end up being created mainly by a collaborative effort of the site visitors.

-Covert: is defined as concealed; secret; disguised.

-Overt: is defined as open and observable; not hidden, concealed, or secret.

-Intelligence Gathering Assignment: An intelligence gathering assignment is a type of online operation which is not directed toward any specific type of illegal activity. The operation may be used as a listening post for general information in a general geographic location where illegal activities are believed to be occurring based on recognized statistic samplings, hot spot designations or High Threat Level designation.

-Public Domain: Any Internet resource that is open and available to anyone.

-Online Undercover Activity: The utilization of an online alias to engage in interactions with a person via social media sites that may or may not be in the public domain (ie: "friending a person on Facebook").

- Entrapment: Entrapment occurs when the Government implants in the mind of a person who is not otherwise disposed to commit the offense the disposition to commit the offense and then induces the commission of that offense in order to prosecute. Entrapment is prohibited.

IV. General Use of Publicly Available Social Networking Sites

A. Precautions and Prohibitions

DOC/CPIC personnel shall abide by the following when using publicly available social networking sites:

1. Members shall not use their official agency e-mail addresses for registration of their personal SNSs.

2. Members should be aware that privacy settings on SNSs are constantly in flux.

3. Members will not represent themselves as members of the DOC/CPIC or Chicago Police Department on their personal websites or SNSs in any manner which brings or is likely to bring discredit upon the Deployment Operations Center (DOC), the Crime Prevention and Information Center (CPIC) and/or the Chicago Police Department. Any member who references the DOC/CPIC or Chicago Police Department in his or her private SNS

use shall make clear that the views expressed are the employee's private views and not those of the DOC/CPIC or the Chicago Police Department.

4. Members who identify themselves as members of the DOC/CPIC, when using SNSs shall comply with the CPIC Privacy Policy, the U.S. and Illinois Constitutions, Federal and State statutes and applicable Municipal Code of Chicago. Chicago Police Department members assigned to the DOC/CPIC will also adhere to all Chicago Police Department Rules and Regulations and applicable Department orders. Members using SNSs shall not knowingly post false or defamatory information regarding the DOC/CPIC, its employees, or members of the public.

5. Members shall treat the official business of the DOC/CPIC as confidential, and may not impart it on SNSs to anyone except those for whom it is intended or under due process of law.

6. The line between public and private, personal and professional communication on SNSs can be unclear. When using SNSs CPIC members should be mindful that their communications may become part of the worldwide electronic domain indefinitely.

7. Members are prohibited from posting, transmitting, disseminating any pictures, audio and/or videos of official DOC/CPIC activities without the express written permission of the Commander of the Deployment Operations Center or his/her designee.

8. Members who become aware of or have knowledge of a posting in violation of the provisions of this policy shall notify the Commander or a supervisor immediately.

9. Any social media participation made pursuant to a DOC/CPIC or Chicago Police Department member's official duties is not considered protected speech under the First Amendment.

10. The DOC/CPIC will gather, store, analyze, and disseminate relevant and appropriate information in conformity with the CPIC Privacy Policy. DOC/CPIC may disseminate applicable information to federal, state, local law enforcement, and private sector partners authorized to receive the information and having a valid need-to-know.

11. Under this policy, the DOC, CPIC fusion center and its members <u>will not</u>:

    a. Actively seek personally identifiable information (PII) without a lawful purpose;

    b. Post any information on social media sites;

    c. Actively seek to connect with other internal/external personal users;

    d. Accept other internal/external personal users' invitations to connect, or;

    e. Interact on social media sites;

    f. Conduct investigations or Department activity off-duty without express authorization of a supervisor in compliance with Chicago Police Department directives regarding overtime.

        - Members should be mindful that that without prior supervisory approval, off-duty monitoring or investigation on the Department's behalf is not authorized nor will such activity be compensated.

12. DOC/CPIC Members are <u>explicitly prohibited</u> from the following:

    a. Posting information containing obscene or sexually explicit language, images, acts and statements or other

forms of speech that ridicule, malign, disparage, or otherwise express bias against any race, any religion, or any protected class of individuals;

b. Posting information that discloses information protected under copyright, is proprietary, or represents an unauthorized disclosure of confidential DOC/CPIC or Chicago Police Department activities;

c. Posting, displaying, or transmitting any communication that discredits or reflects poorly on the DOC/CPIC and the Chicago Police Department, and their respective missions or goals.

B. DOC/CPIC Social Networking Conduct

DOC/CPIC recognizes that Social Networking investigations do not have different requirements when it comes to documenting the investigations. The techniques applied on the internet still require the information be properly collected, preserved and presented.

1. Objectives of social networking Review are to:

- Review social media outlets based on possible threat to public safety or the enforcement of criminal law, or
- Conduct a review that is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents, the resulting justice system response, or the prevention of crime, or
- Review social media based reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal (including terrorist) conduct or activity, or
- Review social media to provide a useful data in crime analysis or in the administration of criminal justice and public safety, and
- Review the source of the information is reliable and verifiable or limitations on the quality of the information are identified, and
- Ensure that the open source information is obtained and collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.
- Determine the nature of the online criminal activity.
- Identify all of the persons involved in the online criminal activity.
- Legally obtain evidence for a search warrant or for prosecution.
- Obtain evidence of the crime from social networking sites.
- Verify investigators online actions.
- Prevent the commission of further crime and apprehend subjects committing crimes through social networking sites.
- Develop leads based on information from other sources.

DEPLOYMENT OPERATIONS CENTER Special Order	Date of Issue 8 April 2015	Effective Date 9 April 2015	No. 15-01
Subject SOCIAL MEDIA POLICY		Amends	
Related Directives		Rescinds	

2. General Authority and Purpose

a. DOC/CPIC personnel are not authorized to engage in undercover activities and covert operations in the theatre of social media without the prior approval of the Commander of the Deployment Operations Center.

b. DOC/CPIC personnel are permitted to make overt inquiries through social media that may be used to further the objective of inquiry into public safety considerations and possible criminal activities by individuals or groups who use social networking to determine whether a full investigation is warranted.

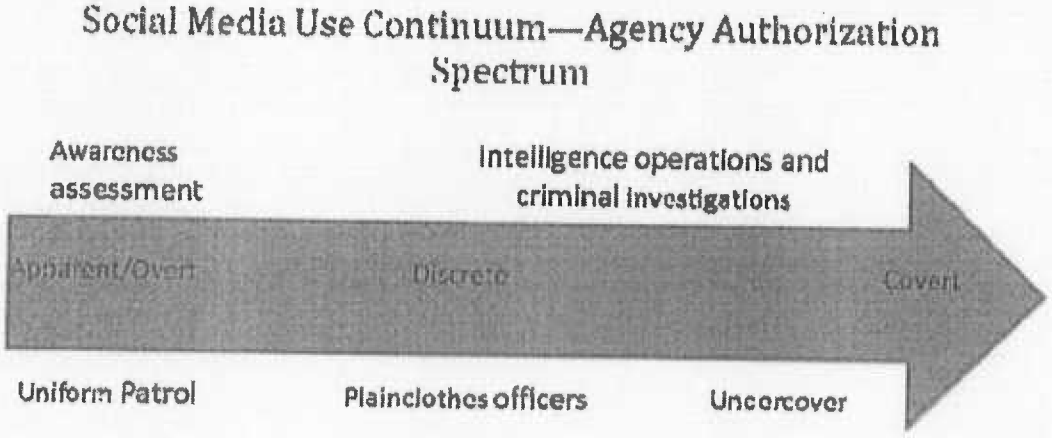
c. DOC/CPIC personnel may assist detectives, investigators and other public safety and law enforcement personnel in providing information obtained through social media regarding crimes when a criminal predicate or public safety issue arises to further the investigative objectives of preventing, solving, and prosecuting crimes. This may include criminal intelligence investigations—i.e., racketeering enterprise investigations and terrorism enterprise investigations—these methods may be used to further the investigative objective of ascertaining such matters as the membership, finances, geographical dimensions, past and future activities, and goals of the enterprise under investigation, with a view to the longer range objectives of detection, prevention, and prosecution of the criminal activities of the enterprise.

d. DOC/CPIC online operations should never be used as a speculative means of search for the existence of a criminal offense, where no other grounds exist to suspect that criminal offenses have been or are being committed. This provision excludes the performance of an Information Gathering Assignment. Any collection of intelligence on specific persons or groups that fall within the guidelines identified in 28 C.F.R. Part 23 need to comply with the Federal rules.

e. DOC/CPIC members will access Public Domain Social networking sites.

f. Some social networking sites, such as Facebook, require a login to be created prior to accessing their sites. On those particular sites that require the creation of a login and provide user personal information, DOC/CPIC members will, with the approval and oversight of a designated DOC/CPIC supervisor or Commander of the Deployment Operations Center, create a moniker or avatar to access the sites.

g. DOC/CPIC members are not allowed to use their personal information or logins to access social media sites for official business.



DEPLOYMENT OPERATIONS CENTER Special Order	Date of Issue 8 April 2015	Effective Date 9 April 2015	No. 15-01
Subject SOCIAL MEDIA POLICY		Amends	
Related Directives		Rescinds	

3. Review of Social Media Access

a. Periodically, the Commander of the Deployment Operations Center may review the conduct of the DOC/CPIC member(s) and others participating in the social media searching and use.

After review if, any center personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding with respect to social networks and internet usage, the Commander of the Deployment Operations Center may:

- Suspend or discontinue access to social media to the violating the center personnel, the participating agency, or the authorized user.
- Apply administrative actions or sanctions as provided by Department General Order 08-01 entitled "Complaint and Disciplinary Procedures" and all addendum of General Order 08-01 in conjunction with the Rules and Regulations of the Chicago Police Department.

Note: If any provisions stated in this policy are in conflict with Chicago Police Department Rules, Regulations and Directives, the Chicago Police Department orders will take precedence.